Härnösands kommun
Kommunstyrelseförvaltningen
Per Jonsson, 0611-34 80 19
per.jonsson@harnosand.se

Datum
2018-02-09

Diarienummer
KS/2017-000672

Riktlinje för informationssäkerhet i Härnösands kommun

Dokumentnamn	Riktlinje för informationssäkerhet i Härnösands kommun		Dokumenttyp Styrdokument	
Fastställd/upprättad av	Kommunstyrelsen		Datum 2018-03-13	Diarienummer 2017-000672
Dokumentansvarig/processägare	Kommunstyrelsen	Version 1:0	Senast reviderad	Giltig t o m 2022-03-13
Dokumentinformation				
Dokumentet gäller för	Samtliga nämnder inom Härnösands kommun			
Annan information				

1. Inledning

Denna riktlinje ger anvisningar om Härnösand kommuns arbete med informationssäkerhet och utgår från den inriktning som fastställts i *Policy för informationssäkerhet*.

Härnösands kommun bedriver verksamhet som har stor betydelse för skyddsvärden som människors liv och hälsa, samhällets funktionalitet, miljö och egendom. Information är av väsentlig betydelse för denna verksamhet och brister i informationssäkerheten kan få betydande konsekvenser. För att genomföra kommunens uppdrag effektivt behövs därför en enhetlig och säker hantering av information, så att dessa skyddsvärden inte äventyras.

Informationssäkerhet är den samlade effekten av organisatoriska, administrativa och tekniska åtgärder för att skydda information mot de hot den kan utsättas för. Informationssäkerhet handlar förenklat om kommunens förhållande till all den information som hanteras. I många fall hanteras information elektroniskt, men lika ofta utanför den digitala världen. Detta dokument gäller för all hantering av informationstillgångar i Härnösands kommun oavsett om den hanteras manuellt eller med IT-stöd.

Arbetet med informationssäkerhet innebär att risker som kan äventyra denna information och ytterst få konsekvenser för det som är skyddsvärt ska identifieras och åtgärdas. Kommunens informationshantering är också en viktig del i samhällets informationssäkerhet. Informationssäkerhet berör alla.

1.1 Syfte och mål

Denna riktlinje ska precisera inriktningen för det arbete som behöver bedrivas på olika nivåer i Härnösands kommun för att förebygga eller begränsa konsekvenserna av risker mot informationssäkerheten. Den beskriver ansvarsområden och arbetssätt.

Riktlinjen anger hur verksamheterna ska agera för att initiera, bibehålla och förbättra informationssäkerheten i Härnösands kommun. De ska vidare ses som ett minimikrav vid utveckling eller anskaffning av nya system och e-tjänster och målet för redan driftsatta sådana.

Till riktlinjen hör metodstöd för arbetet. Riktlinjen kompletteras även av detaljerade anvisningar för arbetet, inklusive vilka krav som bör ställas på hanteringen av olika informationstillgångar, beroende på klassificeringen av dessa.

Utgångspunkten för Härnösand kommuns informationssäkerhetsarbete är att följa den etablerade svenska och internationella standarden inom området, SS-ISO/IEC 27000.

Arbetet med informationssäkerhets syftar till att säkerställa att information som hanteras i kommunens verksamheter, och som är av betydelse för de skyddsvärden som beskrivs i *riktlinjer för kontinuitetshantering* och hanteras med omsorg om informationens konfidentialitet, riktighet, spårbarhet och tillgänglighet. Arbetet bör också vara överensstämmande med såväl kommunens övergripande säkerhets- och beredskapsarbete, som med kommunens förvaltningsmodell för IT.

Information som hämtas in och behandlas inom kommunen ska med stöd av lagar och förordningar samt med hjälp av särskilda åtgärder hanteras så att:

- Informationen är skyddad mot obehörig åtkomst (Konfidentialitet)
- Informationen är korrekt, fullständig och aktuell (Riktighet)
- Informationens användning eller ändring kan härledas (Spårbarhet).
- Informationen finns tillgänglig för de verksamheter som behöver den (Tillgänglighet)

Utgångspunkten är att en klassificering görs av identifierade informationstillgångar, baserat på potentiella konsekvenser om dessa områden inte kan upprätthållas. Till stöd för detta finns metoder som beskrivs närmare i denna riktlinje.

2 Hur arbetet bedrivs

Kraven på ett systematiskt arbete med informationssäkerhet omfattar hela kommunens verksamhet och all information oavsett om den är lagrad digitalt eller analogt. Informationssäkerhetsarbetet kompletterar det mer tekniskt orienterade IT-säkerhetsarbetet i kommunen. De arbetsmetoder som beskrivs i denna riktlinje ska även samordnas med kommunens förvaltningsmodell för IT. För att kunna säkerställa en tillräcklig nivå av informationssäkerhet i kommunens olika verksamheter är det viktigt att informationssäkerhetsarbetet bedrivs systematiskt och långsiktigt.

2.1 Policy för informationssäkerhet

Policyn utgör det styrande dokumentet för informationssäkerhet i kommunen och ger tillsammans med denna riktlinje, inriktning och anvisningar för det samlade informationssäkerhetsarbetet i kommunen. Policyn förtydligar även ansvaret enligt de ledningsstrukturer som presenteras närmare i avsnitt 3.

2.2 Riktlinjer och anvisningar

Denna riktlinje anger ansvarsområden och detaljerade instruktioner för informationssäkerhetsarbetet. Till riktlinjen kopplas dels konkret vägledningsmaterial för arbetet, dels detaljerade anvisningar. Dessa anvisningar bör inkludera exempel på krav som bör ställas inom olika områden vid vissa givna klassificeringsnivåer. Anvisningarna kan även fungera som stöd för att identifiera åtgärdsförslag efter genomförda riskanalyser.

2.4 Löpande arbete

Det löpande informationssäkerhetsarbetet bygger på att informationstillgångar identifieras och klassificeras, med hänsyn taget till möjliga konsekvenser om något av områdena konfidentialitet, riktighet, spårbarhet eller tillgänglighet inte kan upprätthållas. Beroende på klassificeringsnivå krävs vidare arbete, inklusive riskanalyser.

Med informationstillgång avses verksamhetens information och tillgångar relaterade till informationshantering. Exempel på informationstillgångar är:

beslutsunderlag, protokoll, riktlinjer, programvaror, datorutrustning, systemdokumentation, manualer, riskanalyser etc.

Alla informations- och IT-tillgångar ska förtecknas och ha en utsedd ägare. Ytterst ansvarig för samtliga informationstillgångar i verksamheten är verksamhetsansvarig chef, vilken fortsättningsvis benämns verksamhetsägaren.

Ovanstående åstadkoms genom att informationstillgångarna identifieras på ett systematiskt sätt, vilket beskrivs närmare i avsnitt 4.1 nedan.

Verksamhetsägaren ansvarar för att tillgångarna ges rätt skydd utifrån deras betydelse. Utgångspunkt för detta är en klassificering av samtliga informationstillgångar på områdena konfidentialitet, riktighet, spårbarhet och tillgänglighet. Processen för detta beskrivs i avsnitt 4.2.

Verksamhetsägaren avgör slutligen via riskanalyser vilka krav som bör ställas på respektive informationstillgång. Då flera informationstillgångar ofta lagras i samma IT-system är det den högst klassificerade informationstillgången som styr kravställningen, med mindre än att olika informationstillgångar på ett kostnadseffektivt sätt kan separeras, exempelvis genom olika behörighetsnivåer.

Identifiering, klassificering och i förekommande fall riskanalyser med åtgärdsförslag utgör grundläggande moment i informationssäkerhetsarbetet. Nyttan av föreslagna åtgärder skall ställas mot kostnaden av dessa.

Verksamhetsägare ansvarar för att dessa moment genomförs och minst årligen säkerställa att underlag hålls aktuella. För det grundläggande arbetet ansvarar verksamhetsägare, med stöd av utsedda sakkunniga, i enlighet med avsnitt 4 nedan.

Viktiga komplement till det grundläggande informationssäkerhetsarbetet är löpande incidentrapportering samt uppföljning. Detta beskrivs närmare i avsnitt 5 och 6. För löpande incidentrapportering ansvarar verksamhetsägare.

För uppföljning och utbildningsstöd i informationssäkerhetsfrågor svarar kommunsstyrelseförvaltningen.

3 Organisation av informationssäkerhetsarbetet

I detta avsnitt beskrivs övergripande organisation och ansvarsområden för Härnösand kommuns informationssäkerhetsarbete. I avsnittet visas hur arbetet samordnas i förvaltningarna, inklusive med kommunens förvaltningsmodell för IT.

Informationssäkerhetsarbetet i Härnösands kommun bedrivs på tre nivåer: inriktande, samordnande samt operativ. Nedan beskrivs ansvar och roller för dessa tre nivåer.

3.1 Inriktande nivå

Kommunfullmäktige ansvarar för inriktningen av informationssäkerhetsarbetet. Denna inriktning dokumenteras i en informationssäkerhetspolicy.

Kommunstyrelsen leder och samordnar av kommunens säkerhets- och beredskapsarbete och fastställer därför denna riktlinje. Till kommunstyrelsen ska även sammanställningar av inträffade incidenter rapporteras. För denna sammanställning ansvarar kommunstyrelseförvaltningen.

3.2 Samordnande nivå

Kommunstyrelseförvaltningen utgör den samordnande nivån och ansvarar för att upprätta och upprätthålla riktlinjer och anvisningar för informationssäkerhetsarbetet. Till riktlinjen ska även finnas rutinbeskrivningar som utgör stöd för det praktiska informationssäkerhetsarbetet.

Kommunstyrelseförvaltningen ansvarar för att ge stöd och vägledning till kommunens verksamheter på informationssäkerhetsområdet. Kommunstyrelseförvaltningen ansvarar även för att en sammanställning av inträffade incidenter görs och årligen rapporteras till kommunstyrelsen.

3.3 Operativ nivå

Den operativa nivån utgörs av kommunens verksamheter. Verksamhetsägare i dessa ansvarar för det löpande genomförandet av det praktiska informationssäkerhetsarbetet. Arbetet genomförs i enlighet med kommunens förvaltningsmodell för IT, vilket innebär att den som har ansvar för ett visst system också ansvarar för att informationssäkerhetsåtgärder i enlighet med denna riktlinje också vidtas. Till stöd för det praktiska arbetet ska det finnas utsedda sakkunniga.

Informationssäkerhetsarbetet dokumenteras med stöd av rutinbeskrivningar och mallar, som kommunstyrelseförvaltningen tillhandahåller. Verksamhetsägare och/eller den som har ansvaret för ett IT-system ansvarar även för att incidenter rapporteras till kommunstyrelseförvaltningen.

3.4 Förordningar som ställer krav på informationssäkerhet

Krav på informationssäkerhet ställs, utöver i denna riktlinje, även i lagar och förordningar. I detta avsnitt listas exempel på aktuella och tillämpbara regelverk.

Följande lagar, förordningar och föreskrifter ställer direkt eller indirekt krav på informationssäkerheten (exempel):

- Arkivlag (1990:782)
- Föreskrifter och allmänna råd om kommuners risk- och sårbarhetsanalyser (MSBFS 2015:5)
- Föreskrifter om allmänna råd om statliga myndigheters informationssäkerhet (MSBFS 2016:1)
- Föreskrifter och allmänna råd om statliga myndigheters rapportering av it-incidenter (MSBFS 2016:2)
- Förordning (2006:637) om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstidochhöjd beredskap
- Förordning (2015:1053) om totalförsvar och höjdberedskap

- Förvaltningslag (1986:223)
- Kommunallagen (1991:900)
- Lag om offentlig upphandling (2016:1145)
- Lag om kommunal redovisning (1997:614)
- Lag om upphovsrätt till litterära och konstnärliga verk (1960:729)
- Lag om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap (2006:544)
- Offentlighets- och sekretesslagen (2009:400)
- Personuppgiftslagen (1998:204)
- Patientdatalagen (2008:355)
- Säkerhetsskyddsförordning (1996:633)
- Skollag (2010:800)
- Säkerhetsskyddslagen (1996:627)
- Tryckfrihetsförordningen (1949:105)

4 Process för informationssäkerhetsarbete

I detta avsnitt beskrivs hur informationssäkerhetsarbetet konkret bedrivs på operativ nivå. Det grundläggande arbetet utgår från de tre momenten identifiering, klassificering och riskanalys.

4.1 Identifiering av informationstillgångar

Att styra sin informationshantering så att den stödjer verksamheten på ett effektivt och säkert sätt, samtidigt som hänsyn tas till kraven på säker hantering av informationen, kräver såväl ett systematiskt arbetssätt som avvägningar mellan kostnad och nytta. Ett första steg mot en säker informationshantering är att skapa en tydlig bild av vilken information som organisationen nyttjar samt de system, inklusive IT-system, som används för att hantera informationen.

Respektive förvaltnings arbete med identifiering av informationstillgångar utgår från befintliga dokumenthanteringsplaner. Dessa planer skall utgöra en förteckning över den information som verksamheten nyttjar. I dokumenthanteringsplanerna bör även notering göras om i vilket IT-system informationen hanteras. Verksamhetsägaren ansvarar för att dokumenthanteringsplaner finns framtagna och upprätthålls löpande.

Som komplement till dokumenthanteringsplanerna kan en separat förteckning över vilka system för informationshantering som verksamheten nyttjar upprättas. För respektive system görs en inventering av vilka informationstillgångar som hanteras i systemet. För detta ansvarar respektive den som har ansvar för systemet.

Inventeringen bör jämföras med befintliga dokumenthanteringsplanen. Informationstillgångar som inte tidigare upptagits i dokumenthanteringsplanerna förs in i dokumenthanteringsplanen, med en notering om i vilket system informationstillgången hanteras.

Eventuella informationstillgångar som inte är hänförliga till ett specifikt system inkluderas separat i förteckningen.

Resultatet av inventeringen bör bli en komplett förteckning av informationstillgångar i verksamheten, med en tydlig koppling till olika IT-system.

Ovanstående arbete följs upp årligen för att säkerställa att inventeringen är komplett. Särskilda revisioner bör göras vid större verksamhetsförändringar eller nyanskaffningar av IT-system.

4.2 Klassificering av information

För att uppnå rätt grad av säkerhet måste verksamhetens informationstillgångar klassificeras. Förenklat syftar detta till att bedöma och värdera hur viktigt det är att informationstillgångarnas konfidentialitet, riktighet, spårbarhet och tillgänglighet upprätthålls. Potentiella konsekvenser bedöms med stöd av den kriteriemodell som fastsällts i kommunens övergripande riktlinjer för kontinuitetshantering och som omfattar konsekvenser för människors liv och hälsa, miljö, egendom och samhällets funktionalitet. Syftet är alltid att den verksamhet som är beroende av informationen ska kunna upprätthållas ändamålsenligt och effektivt, men med hänsyn taget till behovet av säker informationshantering. Klassningen är vidare beroende av vilka externa krav som ställs på hantering av informationen utefter lagar och förordningar.

Respektive identifierad informationstillgång klassificeras avseende konfidentialitet, riktighet, spårbarhet och tillgänglighet, med utgångspunkt i de konsekvenser som kan uppstå om informationssäkerheten brister. Till stöd finns en fastställd kriteriemodell i kommunens övergripande riktlinjer för kontinuitetshantering. Bedömningen leder till en klassificering enligt fyra skalsteg för respektive område. Dessa skalsteg är:

- Betydande
- Viktig
- Mycket viktig
- Kritisk

I klassificeringsskedet behöver inte konkreta risker beskrivas i detalj. Syftet med kriteriemodellen är att ge en verksamhetsförankrad modell mot vilka potentiella konsekvenser av brister i något av de fyra områdena konfidentialitet, riktighet, spårbarhet och tillgänglighet kan mätas. Om flera potentiella konsekvenser identifieras inom ett område är det de högst värderade som blir styrande för det slutliga klassificeringsbeslutet.

4.2.1 Hantering av informationstillgångar i IT-system

Huvuddelen av kommunens informationstillgångar hanteras i IT-system, tillsammans med andra informationstillgångar. Det är sällan kostnadseffektivt att ställa olika krav på olika delar av samma system. I dessa fall blir de högsta klassificeringsbesluten styrande för systemet som helhet.

4.2.2 Samordna med kontinuitetshanteringsarbete

För området tillgänglighet kan verksamheten kan med fördel nyttja befintligt kontinuitetshanteringsarbete, där beroendeanalyser görs. Hur Härnösands kommun arbetar med kontinuitetshantering specificeras närmare i kommunövergripande riktlinjer för kontinuitetshantering.

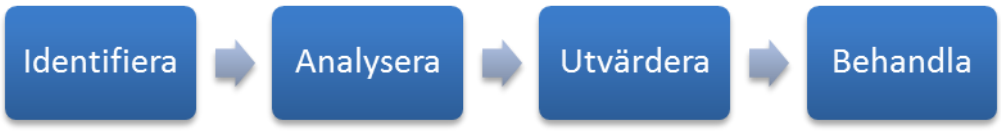
4.3 Riskanalys och riskbehandling

För informationstillgångar där klassificeringsgraden ”mycket viktig” eller ”kritisk” angetts, eller där krav på detta ställs i särskilda lagrum, skall en riskanalys göras. Riskanalysen syftar till att identifiera möjliga händelser som kan påverka förmågan att säkerställa konfidentialitet, riktighet, spårbarhet eller tillgänglighet i informationstillgångarna. Med stöd i riskanalysen kan en prioritering av åtgärder som förebygger eller begränsar konsekvenserna av riskerna göras. Detta utgör ett vidare stöd för informationssäkerhetsarbetet.

Tidigare riskanalyser som genomförts inom ramen för kommunens systematiska säkerhetsarbete samt incidenthistorik kan utgöra ett stöd vid riskanalysen.

Riskanalys enligt nedanstående beskrivning bör även göras vid väsentliga förändringar av befintliga arbetsrutiner som utförs med stöd av mycket viktiga eller kritiska informationstillgångar. Det kan exempelvis handla om förändrade åtkomstrutiner, där åtkomst till IT-system som lagrar känsliga uppgifter möjliggörs från andra platser än den ordinarie arbetsplatsen, eller vid outsourcing av drift av IT-system.

Riskanalysen följer nedanstående processteg:



4.3.1 Identifiera

I detta steg identifieras möjliga händelser som kan påverka verksamhetens förmåga att upprätthålla informationstillgångarnas konfidentialitet, riktighet, spårbarhet eller tillgänglighet, med oacceptabla konsekvenser som följd för människors liv och hälsa, miljö, egendom eller samhällets funktionalitet.

Exempel på sådana händelser är obehörig åtkomst till ett IT-system där handlingar rörande enskilds personliga eller ekonomiska förhållanden lagras, med följd att den enskilde kan lida fysisk eller ekonomisk skada. En sådan obehörig åtkomst kan även ha sekundär påverkan på andra områden, såsom möjlighet att obehörigen ändra uppgifter (riktighet) eller radera dessa (tillgänglighet). Spårbarhet är ofta av betydelse för att kunna säkerställa riktighet och tillgänglighet – genom att identifiera när en ändring gjordes kan exempelvis riktigheten i en informationstillgång bedömas.

4.3.2 Analysera

Med utgångspunkt i identifierade risker analyseras dessa utifrån potentiella konsekvenser, samt sannolikheten för att händelsen inträffar med dessa konsekvenser. Konsekvenser mäts med stöd av samma kriteriemodell som används vid den grundläggande identifieringen av informationstillgångar (se avsnitt 4.1 ovan). Konsekvenser värderas mot olika målområden: människors liv och hälsa, miljö, egendom och samhällets funktionalitet. Konsekvensvärdet för respektive målområde (mätt på en skala 1-4) multipliceras med värdet för sannolikheten, för att ge ett riskvärde. Maximalt riskvärde för respektive målområde är således 16.

4.3.3 Utvärdera

I utvärderingssteget görs en bedömning av om risken kan accepteras eller ej. Risker med riskvärden från 12 och uppåt (höga konsekvenser i kombination med hög sannolikhet) kan generellt ej accepteras. Även risker med konsekvensvärde 4, oaktat sannolikhet, är generellt sett att se som oacceptabla. Avsteg från dessa rekommendationer kan ske, och skälen för detta skall då dokumenteras i riskanalysen.

4.3.4 Behandla

För de risker som i utvärderingssteget ansetts som oacceptabla skall åtgärdsförslag tas fram. Åtgärderna kan syfta till att förebygga risken (exempelvis förhindra obehörig åtkomst till ett IT-system) eller begränsa konsekvenserna av densamma (exempelvis upprättande av regelbundna backup-er som medger återläsning av raderad data).

Till stöd för att upprätta åtgärdsförslag finns detaljerade anvisningar om krav på olika områden, såsom krav på behörighetsstyrning, stark autentisering etc. För dessa anvisningar svarar kommunstyrelseförvaltningen i samråd med IT-avdelningen.

Åtgärdsförslagen utgör beslutsunderlag för exempelvis vidare utveckling av befintliga IT-system.

5 Anvisningar vid nyanskaffning av IT

Vid nyanskaffning av IT-system bör informationssäkerhetsarbetet vara en del av det förberedande arbetet. Vid nyanskaffning ges möjlighet att ställa krav på särskilda informationssäkerhetshöjande åtgärder, som ofta är mer kostsamma att implementera i ett befintligt system. Rutiner avseende upphandling kompletteras därför med ett informationssäkerhetsperspektiv. Nedanstående moment är endast att ses som ett komplement till befintliga upphandlingsrutiner, och åsidosätter inte krav på att upphandlingen utförs affärsmässigt korrekt och objektivt.

5.1 Funktionsbeskrivning

Verksamhetsägare ansvarar för att upprätta en funktionsbeskrivning rörande det tänkta IT-stödet, i enlighet med gällande upphandlingsrutiner.

5.2 Identifiering, klassificering och riskanalys

Verksamhetsägare identifierar de informationstillgångar som bedöms komma att lagras i det tänkta IT-stödet.

En klassificering görs av informationstillgångarna i enlighet med avsnitt 4.2 ovan. För existerande informationstillgångar som redan omfattas av tidigare genomförda klassificeringar görs endast en översyn av befintlig klassificering.

En riskanalys görs för det tänkta IT-stödet, i enlighet med avsnitt 4.3 ovan. I riskanalysen identifieras möjliga åtgärdsförslag.

För arbetet ansvarar verksamhetsägare med stöd av sakkunniga för system, kommunstyrelseförvaltningen (ekonomiavdelningen samt IT-avdelningen) samt av verksamhetsägare utsedda verksamhetsspecialister.

5.3 Formulera informationssäkerhetskrav

Verksamhetsägare ansvarar för att, med utgångspunkt i identifierade åtgärdsförslag och anvisningar för informationssäkerhet, formulera informationssäkerhetskrav till förfrågningsunderlag. Verksamhetsägare ansvarar för att tillämpliga lagrum som kan ställa särskilda krav på informationssäkerhet beaktas, utöver resultatet av riskanalysen. Kraven bör utformas på sådant sätt att en rimlig informationssäkerhetsnivå kan uppnås med hänsyn taget till de eventuella merkostnader för anskaffning, drift och underhåll av IT-stödet som är hänförliga till informationssäkerhetskraven.

Arbetet utförs med stöd av kommunstyrelseförvaltningen (IT-avdelningen och ekonomiavdelningen) samt av verksamhetsägare utsedda verksamhetsspecialister.

5.4 Överlämning till upphandlingsprocess

Identifierade krav inkluderas i ordinarie upphandlingsrutiner.

6 Hantering av informationssäkerhetsincidenter

Ett viktigt verktyg för att upptäcka brister i informationssäkerheten och ytterligare stärka det förebyggande arbetet är löpande incidentrapportering. Med incident menas i detta avseende en händelse som på ett negativt sätt påverkar förmågan att upprätthålla informationstillgångarnas konfidentialitet, riktighet, spårbarhet eller tillgänglighet.

Löpande incidentrapportering syftar till att stärka informationssäkerhetsarbetet genom att ej tidigare identifierade risker och sårbarheter kan belysas. Rapporteringen stöttar även uppföljning och utvärdering av informationssäkerhetsarbetet.

Verksamhetsägare ansvarar för löpande incidentrapportering enligt särskilda anvisningar. Incidenter skall rapporteras:

- Där obehörig åtkomst konstaterats för informationstillgångar som klassats som mycket viktiga eller kritiska ur ett konfidentialitetsperspektiv.
- Där systematiska brister konstaterats avseende riktigheten i informationstillgångar som klassats som mycket viktiga eller kritiska, eller obehörig ändring av sådana tillgångar konstaterats.
- Där bristfällig tillgänglighet i informationstillgångar som klassats som mycket viktiga eller kritiska orsakat betydande påverkan på

verksamheten. Exempel på detta är där avbrott i IT-system pågått under sådan tid att ordinarie verksamhet inte kunnat bedrivas eller krävt mycket stora omställningsåtgärder.

Incidentrapporteringen sammanställs årligen av kommunstyrelseförvaltningen för kommunen som helhet. Se vidare riktlinjer för uppföljning i avsnitt 7.1 nedan.

7 Uppföljning och utbildning

Uppföljning och utbildning är ett centralt ansvar för kommunstyrelseförvaltningen och syftar till att kommunens verksamheter erhåller det stöd som möjliggör en god informationssäkerhetsnivå i verksamheten.

7.1 Uppföljning

Uppföljningen av kommunens informationssäkerhetsarbete skall bedrivas löpande, och inkludera såväl en analys av tillämpningen av denna riktlinje i respektive förvaltning som analys av sammanställd incidentrapportering. Uppföljningen syftar till att ge en översikt avseende kommunens samlade informationssäkerhetsarbete och att identifiera områden där riktlinjer och rutiner kan utvecklas för att förebygga och begränsa konsekvenserna av inträffade informationssäkerhetsincidenter.

7.2 Utbildning

Kommunstyrelseförvaltningen har ett samlat ansvar för informationssäkerhetsarbetet i kommunen, och ansvarar därmed även för att stötta förvaltningarna med utbildningsinsatser och stöd vid genomförandet av det praktiska informationssäkerhetsarbetet. Särskild samordning bör ske mellan kommunens säkerhets- och beredskapsfunktioner och IT-avdelningen för att säkerställa att rutiner och anvisningar upprätthålls med hänsyn tagen till teknisk utveckling, förändringar i lagkrav och andra verksamhetsförändringar som påverkar informationssäkerhetsarbetet.

Bilaga 1 – Anvisningar med krav på informationssäkerhetsområdet

I denna bilaga anges anvisningar med de krav som bör ställas på utformning av verksamhet och teknik för att säkerställa säker hantering av informationstillgångar. Anvisningarna bör ses som en vägledning för utformningen av såväl arbetsrutiner som olika former av IT-stöd. I vissa fall är kraven tvingande. Detta gäller särskilt för informationstillgångar som klassificerats som ”mycket viktiga” eller ”kritiska” med avseende på konfidentialitet, riktighet, spårbarhet eller tillgänglighet. Dessa anvisningar bör särskilt beaktas vid vidareutveckling av befintliga IT-system, eller upphandling av nya system, då möjligheten att på ett kostnadseffektivt sätt säkerställa en högre skyddsnivå är större.

Anvisningarna följer den internationella ISO-standarden 27002, där rekommendationer ges för utformning av informationssäkerhetskontroller.

1.1 Personal och säkerhet

Detta avsnitt ger anvisningar för hur arbetsrutiner och kontroller bör vara utformade för att säkerställa att personalen, såväl egen anställd som inhyrda personalresurser eller konsulter, är lämpade för hantering av konfidentiella informationstillgångar och i övrigt har god kännedom om de rutiner som gäller för säker informationshantering.

Inom detta område bör anvisningar utformas för:

- Bakgrundskontroller och säkerhetsprövning
- Rutiner för introduktion och utbildning i informationssäkerhetsfrågor vid nyanställning
- Rutiner för avveckling av konton, inklusive behörigheter till IT-system där konfidentiell information lagras, och återlämning av IT-utrustning vid avslutad anställning
- Regler för användning av kommunens IT-system, inklusive datalagring, e-posthantering och hantering av mobiltelefoni
    - För e-posthantering bör särskild vikt läggas vid att upprätta rutiner för hantering av handlingar i enlighet med offentlighetsprincipen (Tryckfrihetsförordningen (1949:105) kap 2.) samt befordran av information som innehåller konfidentiella uppgifter. Se vidare avsnitt 1.2 avseende hantering av allmänna handlingar.
- Riktlinjer för lagring av informationstillgångar utanför Härnösands kommuns IT-miljö (så kallade molntjänster).
- Riktlinjer för installation av applikationer i Härnösands kommuns IT-miljö.
- Riktlinjer för hantering av informationstillgångar som omfattas av datalagringsdirektivet (GDPR).

1.2 Hantering av tillgångar

Detta avsnitt ger anvisningar för hur Härnösands kommun bör hantera såväl informationstillgångar som fysiska informationsbärare, inklusive datorer och annan stöldbegärlig utrustning.

Inom detta område bör anvisningar utformas för:

- Märkning och hantering av stöldbegärlig egendom.
- Hantering av flyttbara lagringsmedia (USB-stickor, mobiltelefoner och annan utrustning med stor lagringkapacitet)
- Hantering av allmänna respektive icke allmänna handlingar i enlighet med offentlighetsprincipen (se vidare Tryckfrihetsförordningen, kap 2), inklusive gallring och arkivering.
- Markering och hantering av informationstillgångar som klassificerats som viktiga, mycket viktiga eller kritiska på området konfidentialitet, eller som i övrigt omfattas av sekretess i enlighet med Offentlighets- och Sekretesslagen (2009:400)
    - Särskild vikt bör läggas vid anvisningar för hur sekretessmarkerade handlingar förvaras och befordras.

1.3 Fysiskt skydd

Detta avsnitt ger anvisningar för hur Härnösands kommun bör säkerställa att informationstillgångar med hög klassificering avseende konfidentialitet, riktighet eller tillgänglighet fysiskt skyddas mot obehörig åtkomst.

Inom detta område bör anvisningar utformas för:

- Skalskydd och tillträdesbegränsningar, inklusive anvisningar för upprättande av passerkontrollsystem och/eller nyckelhantering samt loggning av tillträde till lokaler där högt klassificerade tillgångar förvaras.
- Fysiskt skydd av informationstillgångar, inklusive IT-utrustning, mot yttre påverkan på grund av brand, vattenläckage eller annan störning i tekniska försörjningssystem.
    - Särskild vikt bör läggas vid anvisningar för utformning av säkra driftlokaler (serveranläggningar med mera).

1.4 Operativt skydd

Detta avsnitt ger anvisningar för hur Härnösands kommun bör säkerställa skydd av IT-drift i enlighet med kommunens förvaltningsmodell för IT.

Inom detta område bör anvisningar utformas för:

- Driftrutiner inklusive ansvar för dokumentation
- Ändringar i driftmiljö (ändringshantering)
- Upprättande av servicenivåavtal
- Rutiner för extern drift och lagring av informationstillgångar
    - Särskild vikt bör läggas vid att säkerställa att extern drift och lagring av informationstillgångar sker i enlighet med lagkrav

samt med beaktande av leverantörens förmåga att skydda informationen mot obehörig åtkomst, förändring eller radering. Vidare bör de krav på lämplighetsprövning som beskrivs i avsnitt 1.1 om personal beaktas även vad avser leverantörens personal.

- Skydd mot skadlig kod
- Säkerhetskopiering samt redundant drift och lagring av informationstillgångar som klassats som mycket viktiga eller kritiska ur ett tillgänglighetsperspektiv.
- Upprättande och vidmakthållande av loggar för att säkerställa spårbarhet avseende åtkomst och hantering av informationstillgångar

1.5 Åtkomst- och behörighetsstyrning

Detta avsnitt ger anvisningar för hur Härnösands kommun bör säkerställa skydd mot obehörig åtkomst av informationstillgångar som lagras i IT-system.

Inom detta område bör anvisningar utformas för:

- Behörighetsadministration (se även avsnitt 1.1 om avveckling av behörigheter vid upphörande av anställning) avseende IT-system
- Lösenordshantering
- Autentisering av användare
- Åtkomst till nätverk och IT-system, inklusive spärrande av användarkonton vid misstänkt obehöriga åtkomstförsök.
- Kryptering av konfidentiell information
- Åtkomst av IT-system från platser utanför Härnösands kommuns IT-miljö
- Rutiner och arbetssätt avseende mobil åtkomst och distansarbete